METHOD AND APPARATUS FOR ENCRYPTING AND COMPRESSING MULTIMEDIA DATA

BACKGROUND OF THE INVENTION

Field of the Invention

[01] The present invention relates generally to a method and apparatus for encrypting and compressing multimedia data, and more particularly to a method and apparatus for encrypting and compressing multimedia data, which transforms and compresses multimedia data through a certain encryption key in a process of compressing the multimedia data to record and transmit the multimedia data, and which encrypts the multimedia data to allow the multimedia data to be decoded using only the encryption key used in the compressing process. The present application is based on Korean Patent Application No. 2002-72813, which is incorporated herein by reference.

DESCRIPTION OF THE RELATED ART

[02] Moving Picture Experts Group (MPEG) standards are international standards for methods of compressing and storing, and transmitting moving images and audio data, and, methods of decompressing, processing and coding compressed information. The MPEG standards include MPEG-1,

MPEG-2 and MPEG-4. Of the MPEG standards, MPEG-1 (ISO/CEI 11172), which is the most basic method of compressing multimedia data, eliminates or transforms duplicated information and compresses moving image signals by applying statistical properties to the remaining or transformed multimedia data.

[03] MPEG standards use Discrete Cosine Transform (hereinafter referred to as "DCT") and quantization to remove spatial redundancy, use Differential Pulse Code Modulation (DPCM) to remove temporal redundancy, and additionally use entropy encoding including Run Length Coding (RLC) and Hoffmann coding.

[04] Additionally, MPEG standards basically include Groups Of Pictures (GOPs) each of which is a set of frames. Each of the GOPs includes an Intra-frame (I-frame), a forward Predicted frame (P-frame) and a Bi-directional predicted frame (B-frame).

[05] Recently, as a wireless communication technology has developed and a mobile communication technology has been widely used, multimedia services based on the compressing method have been offered, and therefore the security of data provided through the multimedia services has been further required.

[06] That is, corresponding services should be provided only to users having service use rights. For example, movies are transmitted only to users

having paid certain fees, or image information is transmitted only to users having rights by which they participate in secret conferences.

[07] The Data Encryption Standard (hereinafter referred to as "DES") adopted as an international standard algorithm in 1997, is generally used as an encryption algorithm.

[08] DES is a block encryption algorithm that processes a block unit of plain text using a symmetric key, and is used to transmit and reproduce compressed multimedia data for providing secure multimedia services.

[09] US Patent No. 6,021,199 entitled "Motion picture data encrypting method and computer system and motion picture data encoding/decoding apparatus to which encrypting method is applied" discloses a method of encrypting multimedia data using an MPEG compression method that selectively encrypts the I-frames of MPEG data through DES, using the property of the I-frame to include original image information, thus reducing the amount of data.

[10] A process of encrypting multimedia data using such an MPEG compression method is carried out as shown in Figs. 1 and 2.

[11] That is, many of the values of an 8 x 8 block become 0 through DCT and quantization processes, as shown in Fig. 1.

[12] To efficiently process the frame data described above, the values of Differential Coefficients (hereinafter referred to as "DC coefficients") and

Amplitude Coefficients (hereinafter referred to as "AC coefficients") are read in a zig-zag order, for example, in the order of DC, AC1, AC2, . . ., and AC63, compressed through an entropy encoding process (100), and encrypted through the DES encryption process (200).

[13] Additionally, as shown in Fig. 2, a multimedia data producer receives a public key sent from multimedia data receivers at step 1, and generates a symmetric key needed to decode encrypted multimedia data provided through multimedia services, encrypts the generated symmetric key using the public key sent from the receiver and sends the symmetric key to the receiver at step 2.

[14] The producer periodically changes the symmetric key used in the DES and therefore improves the security of data at step 3.

[15] A method of encrypting MPEG data using the shared symmetric key according to a DES algorithm requires resources for processing encrypting and decoding processes because the encrypting and decoding processes are complicated.

[16] Additionally, since the method cannot improve a data compression ratio of multimedia data, the method is not suitable for real time multimedia services provided to wireless mobile terminals.

[17] Accordingly, there have been demands for a multimedia security system that efficiently handles limits of the bandwidth resources of a

wireless network environment and limits of the computation resources of a mobile terminal.

SUMMARY OF THE INVENTION

[18] Accordingly, the present invention has been made keeping in mind the above problems occurring in the related art, and an object of the present invention is to provide a method and apparatus for encrypting and compressing multimedia data, in which entropy encoding is carried out depending on a certain encryption key at the time of entropy encoding in an MPEG compression process, and multimedia data is encrypted and compressed depending on transformed encoded results.

[19] Another object of the present invention is to provide a method and apparatus for encrypting and compressing multimedia data, in which a coding process is performed using certain symmetric keys, thus improving a data compression ratio.

[20] The method for encrypting and compressing multimedia data according to the present invention includes the steps of: creating DCT coefficients by applying input multimedia data to a DCT unit, and quantizing the created DCT coefficients; encrypting and compressing DC and AC coefficients transformed by transforming encoded DC and AC coefficients depending on a certain encryption key at the time of entropy encoding quantized DC and AC coefficients of the quantized DCT coefficients; and

Huffmann coding the encrypted DC and AC coefficients using a Huffmann table and outputting the coded DC and AC coefficients.

[21] Additionally, the apparatus for encrypting and compressing multimedia data according to the present invention includes: a DCT unit for creating DCT coefficients including AC and DC coefficients by DCT transforming multimedia data into discrete signals; a quantization unit for quantizing the created DCT coefficients using a quantization table; and an entropy encryption encoding unit for encrypting quantized AC and DC coefficients by entropy encoding the quantized AC and DC coefficients using a certain encryption key.

BRIEF DESCRIPTION OF THE DRAWINGS

[22] The above and other objects, features and other advantages of the present invention will be more clearly understood from the following detailed description taken in conjunction with the accompanying drawings, in which:

[23] Fig. 1 is a view showing a schematic construction of a conventional apparatus for encrypting multimedia data through DES using an MPEG compression method;

[24] Fig. 2 is a view showing a schematic construction of a conventional system for encrypting multimedia data through the DES using an MPEG compression method;

[25] Fig. 3 is a view showing a schematic construction of an apparatus for encrypting and compressing multimedia data according to the present invention;

[26] Fig. 4 is a flowchart showing a method for encrypting and compressing multimedia data according to the present invention;

[27] Fig. 5 is a view showing a schematic construction of a system including the encrypting and compressing apparatus according to the present invention;

[28] Figs. 6a to 6c are views showing an original image and encrypted and compressed results thereof according to the present invention; and

[29] Figs. 7a to 7c are views showing another original image and encrypted and compressed results thereof according to the present invention.

DESCRIPTION OF THE EXEMPLARY EMBODIMENTS

[30] Hereinafter, a method and apparatus for encrypting and compressing multimedia data according to embodiments of the present invention will be described in detail with reference to the attached drawings.

[31] A method and apparatus for encrypting and compressing multimedia data is implemented based on an H.261 moving picture compression algorithm of MPEG-1. The meanings of terms for explaining compression processes, and hierarchical structures are defined in the H.261 moving picture compression algorithm of MPEG-1.

[32] Accordingly, when the method and apparatus for encrypting and compressing multimedia data are explained, the detailed description of the meanings of terms, hierarchical structures and various kinds of parameters, which may obscure the point of the present invention, will be omitted.

[33] Additionally, in the present invention, DC and AC coefficients are encrypted by different methods through the use of symmetric keys. The DC coefficient is encrypted by a method in which codes are changed according to an encryption key, as provided in "An Efficient MPEG Video Encryption Algorithm" by Shi and Bhargava. The AC coefficient is encrypted by a method additionally performing lossy compression.

[34] The apparatus for encrypting and compressing multimedia data will be described in detail with reference to Fig. 3.

[35] As shown in Fig. 3, the apparatus for encrypting and compressing multimedia data according to the present invention includes a DCT unit 110 that creates DCT coefficients including AC and DC coefficients by DCT transforming input multimedia data into discrete signals, a quantization unit 150 that quantizes the created DCT coefficients using a quantization table 130, and an entropy encryption encoding unit 170 that encrypts quantized AC and DC coefficients by entropy encoding the quantized AC and DC coefficients using a certain encryption key.

[36] The entropy encryption encoding unit 170 includes a DPCM unit 171 that pulse modulates the quantized DC coefficient of the DCT coefficients,

an RLC unit 173 that scans the quantized AC coefficient of the DCT coefficients in a zig-zag run manner, an encryption unit 175 that encrypts the DC and AC coefficients using a Variable Length Code (VLC) and a Variable Length Integer (VLI) of each of the DC and AC coefficients obtained by the DPCM unit 171 and the RLC unit 173, and a Huffmann coding unit 179 that Huffmann codes the encrypted DC and AC coefficients using a Huffmann table 177.

[37] The method for encrypting and compressing multimedia data using the apparatus described above includes the steps of: creating a DCT coefficient by applying input multimedia data to the DCT unit 110, and quantizing the created DCT coefficients; encrypting and compressing DC and AC coefficients transformed by transforming encoded DC and AC coefficients depending on a certain encryption key at the time of entropy encoding quantized DC and AC coefficients of the quantized DCT coefficients; and Huffmann coding the encrypted DC and AC coefficients using the Huffmann table 177 and outputting the coded DC and AC coefficients.

[38] The step of encrypting and compressing the DC and AC coefficients includes the steps of: differential pulse code modulating on the quantized DC coefficients and performing RLC of the quantized AC coefficient; determining the encryption key of the AC and DC coefficients and a random constant r indicating a start bit of the encryption key, using variable length

information, which is a VLC and a VLI, of each of the DC and AC coefficients obtained through the DPCM and the RLC; and encrypting the AC and DC coefficients using the determined encryption key.

[39] The step of encrypting the DC coefficient includes the steps of: determining whether a value of an r-th bit is "1" in the determined encryption key of the DC coefficient; and transforming the DC coefficient by performing an exclusive logical sum operation between the VLC of the DC coefficient and 11111111 if the determination result is "1".

[40] The step of encrypting the AC coefficient includes the steps of: determining whether a value of an r-th bit is "1" in the determined encryption key of the AC coefficient; right-shifting the VLI of the AC coefficient if the determination result is "1"; determining the VLC of the AC coefficient through the right-shifted VLI using the Huffmann table; and transforming the AC coefficient using the determined VLC and VLI.

[41] The encryption key includes two symmetric keys, and the symmetric keys are VLCs of the AC and DC coefficients, respectively. Accordingly, the DC and AC coefficients are entropy encoded on the basis of the VLC of each of the DC and AC coefficients, and variable encoded results are compressed to be decoded by only the VLC.

[42] An embodiment of the method for encrypting and compressing multimedia data will be described in detail with reference to the attached drawings.

[43] For example, a vector matrix of (DC, AC1, AC2, . . ., AC63) according to a zig-zag order is shown in the following Table 1.

Table 1

3	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	7	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Table 2

Range of DIFF(k) value	Bit size (m)	Huffmann code
0	0	00
-1, 1	1	010
-3, -2, 2, 3	2	011
-7, . . .,-4, 4, . . .,7	3	100
	. . .	
-255, . . ., -128, 128, . . .,255	8	1111110

[44] An 8 x 8 block is zig-zag scanned using the DC and AC coefficients. The DC coefficient is encoded to a VLC indicating a minimum bit size for expressing the DC coefficient using the Huffmann Table, and a VLI indicating a bit corresponding to the VLC in the DC coefficient.

[45] According to the embodiment, since the DC coefficient is "3", the minimum bit size for expressing "3" is determined to be "2" with reference to Table 2 (Huffmann Code for the DC coefficient).

[46] Accordingly, the VLC of the DC coefficient is 2(011), and the VLI indicating a bit corresponding to "2" of the bit size of the VLC from the least significant bit of 011 expressing "3" of the DC coefficient becomes 11.

[47] Additionally, an entropy encoded result of the DC coefficient including the VLC and the VLI is 01111.

[48] The AC coefficient is a series of bit stream, in which the number of repetitions I of "0" and a bit size m for expressing a non-zero number is compressed using RLC. According to the present invention, the number of repetitions I is "7", and the bit size m for expressing non-zero number "7" is "3" with reference to the following Table 3 (AC coefficient magnitude category for bit size table).

Table 3

Bit size	Range of AC value
0	0
1	-1,1
2	-3,-2,2,3
3	-7,. . ., -4,4, . . .,7
4	-15, . . .,-8,8, . . .,15
	. . .
10	-1023,. . .,-512,512,. . .,1023

Table 4

Run/Level	Bits	VLC
7/1	8	11111010
7/2	12	11111111011
7/3	16	1111111110101110
7/4	16	1111111110101111
7/5	16	1111111110110000
7/6	16	1111111110110001
7/7	16	1111111110110010
7/8	16	1111111110110011
7/9	16	1111111110110100
7/A	16	1111111110110101

[49] Accordingly, if the VLC corresponding to (7, 3) is determined using Table 4 (Typical AC Huffmann Code Table), the VLC of the AC coefficient is 1111111110101110.

[50] Since the VLI indicating a bit size of "3" for expressing "7" in the VLC is 110, an entropy encoded result of the AC coefficient including the VLC and the VLI is 11111111110101110110.

[51] That is, if the VLC and VLI of each of the DC and AC coefficients are created through the DPCM unit 171 and the RLC unit 173 of the entropy encryption encoding unit 170 according to the processes, encryption and compression processes are carried out using the VLCs and VLIs.

[52] Encryption and compression processes using the VLC and VLI of each of the DC and AC coefficients will be described with reference to Fig. 4.

[53] As shown in Fig. 4, the VLC and VLI of each of the DC and AC coefficients are generated by performing DPCM and RLC of the quantized DC and AC coefficients, respectively, and an encryption key (hereinafter referred to as "first and second symmetric keys") and a random constant r indicating the start bit of the first or second symmetric key 2 are determined using the generated VLC and VLI of each of the DC and AC coefficients at step S1. The first and second symmetric keys are determined by the VLCs of the DC and AC coefficients, and the key 1 is defined as the VLC of the DC coefficient and the key 2 is defined as the VLC of the AC coefficient.

[54] If the first and second symmetric keys and the random constant are determined, it is determined whether a key corresponds to the DC coefficient at step S2.

[55] If a key corresponds to the DC coefficient as a result of the determination of step S2, it is determined whether the value of a bit corresponding to the random constant designated in the first symmetric key is "1" at step S3. If the value of the bit is "1", an exclusive logical sum (XOR) operation between the VLI of the DC coefficient and 11111111 is performed at step S4.

[56] An encoded DC coefficient is transformed depending on a value of the VLI varied by the XOR operation with 11111111 at step S5.

[57] That is, if it is assumed that the random constant is "2" and applied to the embodiment, and a value of a second bit of the VLI is "1" in the DC coefficient, in which the VLC is 011 and the VLI is 11, so that a result of the XOR operation with 11111111 is 11111100.

[58] In the XOR operated result, the VLI constructed by extracting a bit corresponding to "2" of the bit size of the VLC becomes 00.

[59] Accordingly, the encoded DC coefficient is transformed to 01100 by the variable VLI.

[60] If a key does not correspond to the DC coefficient as a result of the determination of step S2, it is determined whether the value of the bit corresponding to the random constant designated in the second symmetric key is "1" at step S6. If the value of the bit is "1", the VLI of the AC coefficient is right-shifted at step S7.

[61] An encoded AC coefficient is transformed depending on the value of the VLI varied by the right-shifting at step S8.

[62] That is, according to the embodiment, since the second bit of the VLI is "1" in the AC coefficient in which the VLC is 1111111110101110 and the VLI is 110, the VLI becomes 011 if the VLI is right-shifted.

[63] Since the VLI is 3(011) as the result of step S8, "2" of the minimum size bit for expressing "3" can be applied to the AC coefficient, so that the AC coefficient is transformed from (7, 3) to (7, 2).

[64] Accordingly, if Table 4 is searched for the VLC corresponding to (7, 2), the VLC is 111111110111, and the VLI constructed by extracting a bit corresponding to the bit size of the VLC is 11.

[65] The encoded AC coefficient transformed by the variable VLI is 1111111011111.

[66] As described above, compressed AC and DC coefficients are encrypted so that they can be decoded through only the first and second symmetric keys, which are the encryption key.

[67] If the first and second symmetric keys are determined through the processes and multimedia data is encrypted and compressed, the multimedia data producer receives a public key from the multimedia data receiver B, and the first and second symmetric keys are encrypted through the public key of the multimedia data receiver B and sent to the receiver, as shown in Fig. 5.

[68] Multimedia data receivers decode the multimedia data using their own private keys so that compressed multimedia data provided through the multimedia services can be decoded.

[69] That is, since the multimedia data is encoded depending on the first and second symmetric keys and the random constant r, multimedia data

cannot be decoded and reproduced if a user does not know the first and second symmetric keys, so that security of the multimedia data can be ensured.

[70] The multimedia data producer periodically changes the first and second symmetric keys and the random constant r to increase security of the multimedia data. The random constant r is changed more often than the first and second symmetric keys, so that a time T at an interval of which the first and second symmetric keys are changed is longer than a time t at an interval of which the random constant r is changed.

[71] Additionally, the bit stream of the AC coefficient is reduced and a data compression ratio is improved through the above described encrypting and compressing processes according to the present invention. In the present invention, the AC coefficient is transformed from (7, 3) to (7, 2) through the above described encoding process using the second symmetric key, so that the AC coefficient can be reduced by 5 bits.

[72] Accordingly, when it is considered that the 8 x 8 block is a part of a macro block of a slice layer in a frame, a considerable compression effect can be expected in a total moving image file.

[73] Such encrypted and compressed results will be described with reference to Figs. 6a to 6c and Figs. 7a to 7c. Figs. 6a and 7a illustrate original images, and Figs. 6b and 7b illustrate encrypted and compressed results of the original images.

[74] Decoded results of the encrypted and compressed images using the first and second symmetric keys according to the present invention are shown in Figs. 6c and 7c.

[75] As shown in Figs. 6c and 7c, effective encoded and decoded results can be obtained through simple operations, such as XOR operation and right-shifting, according to the present invention.

[76] Additionally, a conventional data compression ratio compared to a data compression ratio according to the encrypted and compressed results of the present invention shown in Figs. 6a to 6c and 7a to 7c are arranged in Table 5.

[77] From Table 5, it is confirmed that the data compression ratio according to the present invention will be remarkably higher than the conventional data compression ratio.

Table 5

	Figs. 6a to 6c		Figs. 7a to 7c	
	Compression ratio	Size	Compression ratio	Size
MPEG Standard	81:1	31231 (bytes)	40:1	174387
Present invention	118:1	21455	52:1	133968

[78] Table 6 illustrates overhead required to calculate a corresponding frame. In the case of Figs. 6a to 6c, 0.05746 seconds is additionally taken

compared to a compression method according to the MPEG standard, so that the overhead of 1.32% is shown. In the case of Figs. 7a to 7c, 0.039373 seconds is additionally taken compared to the compression method according to the MPEG standard, so that the overhead of 0.88% is shown.

[79] From the results, it can be appreciated that the generated overhead according to the present invention is a negligible small value.

Table 6

	Figs. 6a to 6c	Figs. 7a to 7c
MPEG standard	3.321732(second per frame)	3.564230
Present invention	3.378378	3.603603

[80] As described above, according to the present invention, encrypting and decoding processes are not complicated because input multimedia data is encrypted using entropy encoding results varied depending on a certain encryption key, so that the present invention is suitable for multimedia services for mobile terminals and a data compression ratio is high, thus being effective in multimedia processing on a wireless communication.

[81] Although the exemplary embodiments of the present invention have been disclosed for illustrative purposes, those skilled in the art will appreciate that various modifications, additions and substitutions are possible, without departing from the scope and spirit of the invention as disclosed in the accompanying claims.